

Prüfung grösserer Zahlen auf ihre Eigenschaft als Primzahlen.

Von P. Seelhoff.

Die unten stehende Tabelle enthält eine Zusammenstellung von binären quadratischen Formen, deren Determinante negativ und deren mittlerer Coefficient Null ist, während die äusseren Coefficienten relative Primzahlen sind. Da für die Charaktere, welche ihnen entsprechen, keine andere reducirte Form mit derselben Determinante existirt, so muss sich jede Primzahl N mit den entsprechenden Charakteren entweder durch eine einzige dieser Formen darstellen lassen, wenn diese allein steht oder alternativ durch eine von zweien, wenn sie gepaart vorkommen oder durch eine von vieren, wenn sie zu vieren verbunden sind. Da die Determinanten theilweise verhältnismässig gross sind, so bieten sie ein gutes Mittel dar, um selbst sehr grosse Zahlen ohne zu grossen Aufwand von Arbeit daraufhin zu prüfen, ob sie Primzahlen sind und auch, um die Faktoren zu bestimmen, falls sie zusammengesezt sind, letzteres natürlich nur in dem Falle, wenn die Determinante quadratischer Rest der Zahl, mithin auch ihrer sämmtlichen Faktoren ist. Die Tabelle enthält nur die Formen für Zahlen von der Form $8n+1$, und man wird bei genauerer Prüfung finden, dass diese Formen alle möglichen Fälle decken.

Über die Einrichtung der Tabelle ist Folgendes zu bemerken. Da es erforderlich ist, dass die Determinante quadratischer Rest der zu prüfenden Zahl N ist, so handelt es sich zunächst darum, wie sich die einzelnen Primzahlen, welche erstere constituiren, zu N oder umgekehrt, wie sich N zu den Primzahlen in dieser Beziehung verhält. Ist nun N congruent einem quadratischen Reste nach dem Modulus α, so ist α in der Tabelle unter $+$ eingetragen, im anderen Falle unter $-$. So findet man *z. B.* in der Zeile 33 die Primzahl 3 unter $-$ und 5 unter $+$, in der Rubrik Formen für diese die einzelne Form $(5, 9)$ oder vollständig $(5, 0, 9)$ und die gepaarten Formen $\begin{pmatrix} 9, & 20 \\ 5, & 36 \end{pmatrix}$ d. h. ist $N \equiv 1\ (3)$ und $N \equiv 1$ oder $4\ (5)$, so ist N eine Primzahl, wenn es sich nur auf eine einzige Art durch die Form $(5, 0, 9)$ darstellen lässt, oder wenn man die gepaarten Formen zur Prüfung wählt, wenn nur eine Darstellung entweder durch $(9, 0, 20)$ oder $(5, 0, 36)$ möglich ist. In

Zeile 10 findet man, dass 3 und 5 beide unter + stehen und die zugehörigen Formen sind 4 an der Zahl. Ist also $N \equiv 1\,(3)$ und $\equiv 1$ oder $4\,(5)$, so ist es eine Primzahl, wenn es sich durch eine der vier Formen einmal darstellen lässt. Sowohl in dem ersten wie in dem zweiten Falle gilt ferner, dass wenn man keine Darstellung oder mehr als eine fur N findet, dieses nur eine zusammengesetzte Zahl sein kann, und dass, wenn sich mehr als eine Darstellung findet, aus diesen Darstellungen die Faktoren von N abgeleitet werden können.

Um zugleich zu zeigen, wie vortheilhaft selbst die zu vieren verbundenen Zahlen zur Prüfung sehr grosser Zahlen verwandt werden können, wähle ich für ein erläuterndes Beispiel die Zahl $N = 2^{31} - 1 = 2147470249$. Bekanntlich hat Euler diese Zahl zuerst untersucht und zwar vermittelst Division durch die einzig möglichen Primzahlen von der Form $248z + 1$ und $248z + 63$ bis zu $\sqrt{N} = 46339$ und dieselbe als Primzahl bestimmt.

Wählen wir zu demselben Zwecke eine Form, welche der Tabelle fur die Zahlen von der Form $8n + 7$ angehört. Für $N \equiv 1\,(3)$, $\equiv 1\,(7)$, $\equiv 1\,(11)$, $\equiv 7\,(29)$ hat man die verbundenen Formen (1, 0, 13398), (22, 0, 609), (42, 0, 319), (58, 0, 231). Eine und nur eine von diesen muss eine einzige Darstellung von N geben, falls dieses eine Primzahl ist; dann ist jeder Versuch mit den andern noch übrigen Formen zwecklos. Würde sich keine Darstellung für sämmtliche 4 Formen ergeben, so wäre N keine Primzahl, ebenso nicht, wenn sich für dieselbe Form mehr als eine Darstellung herausstellte. Nun giebt die erste Form (1, 0, 13398) keine Darstellung, ich gehe daher gleich zu der zweiten (22, 0, 609) über, um an ihr das ganze Verfahren im Allgemeinen auseinanderzusetzen. Da also $22x^2 + 609y^2 = N$ sein soll, so muss N in solche zwei Theile zerlegt werden, von denen der eine ein Multiplum von 22, der andere ein solches von 609 ist. Setzt man demgemäss

$$22a + 609b = 2147483647,$$

so ist

$$a = 97612810 - 609k$$
$$b = 3 + 22k.$$

Da $a = x^2$ ist, so müssen die Werthe α für x so genommen werden, dass $97612810 - \alpha^2$ durch 609 theilbar ist. $609 = 3.7.29.97612810 \equiv 1\,(3)$, $\equiv 1\,(7)$, $\equiv 28\,(29)$ und da $1^2 \equiv 1\,(3)$, $1^2 \equiv 1\,(7)$, $12^2 \equiv 28\,(29)$ ist, so ist $x = 3t \pm 1 = 7u \pm 1 = 29v \pm 12$. Hieraus folgen 8 Werthe für x, nämlich $609n + 41$, 104, 244, 302, 307, 365, 505, 568 bis zu der Grenze $\sqrt{97612810} = 9879$. Setzt man diese für x ein, bildet k und hieraus b, so ist eine Darstellung gefunden, wenn b eine Quadratzahl und das zu x gehörige $y = \sqrt{b}$. Übrigens kommen alle geraden Werthe für x nicht in Betracht, weil diese in $22x^2 + 609y^2 = N$ nur Zahlen von der Form $8n + 1$ liefern,

und von den ungeraden fallen noch diejenigen mit der Endziffer 5 aus, da im Voraus zu ersehen ist, dass sie keine Quadratzahl für b hervorbringen können. Für $x = 7001$ findet sich dann $b = 1755625$ und $y = 1325$, also $22.7001^2 + 609.1325^2 = 2147483647$. Da sich für diese Form keine weitere Darstellung ergiebt und da die Zahl somit eine Primzahl ist, so ist die Untersuchung abgeschlossen.

*Als Beispiel für eine zusammengesetzte Zahl diene $N = 165580141$. Da $N \equiv 6\,(7), \equiv 1\,(11), \equiv 12\,(13)$, so kann man die geparten Formen (14, 0, 143) und (26, 0, 77) benutzen und erhält mit der ersten:

$$14.1399^2 + 143.983^2 = 165580141$$
$$14.3089^2 + 143.473^2 = \quad ``$$

Sind aber α, β und γ, δ zwei Darstellungen der Zahl N durch die Form (m, n), so setze man $\frac{p}{q} = \frac{\alpha \pm \gamma}{\beta \pm \delta}$, und reducire die sich hieraus ergebenden Brüche, so dass p gleich dem Zähler und q gleich dem Nenner ist. Dann bilde man weiter den Bruch $\frac{r}{s} = \frac{mp^2}{nq^2}$ und reducire, so dass hier r gleich dem Zähler und s gleich dem Nenner wird. Dann ist $f = r + s$, oder, wenn dies eine gerade Zahl ist, die Hälfte hiervon ein Faktor, von N.

Also in unserem Beispiele $\frac{p}{q} = \frac{3089 - 1399}{983 - 473} = \frac{169}{51}\ \frac{r}{s} = \frac{14.169^2}{143.51^2}\,.\,f = 59369.$

Aus $\frac{p}{q} = \frac{3089 - 1399}{983 + 473}$ findet man den zweiten Faktor 2789, mithin

$$2789.59369 = 165580141.$$

Die gewählte Zahl ist das 41[te] Glied der Reihe

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21\ \ldots$$

Zum Schlusse meiner Mittheilung möchte ich noch darauf hinweisen, dass neben den Tabellen für die Formen, von welchen die hier gegebene zunächst nur als Beispiel dienen soll, eine genügend weit reichende Tafel der Quadrat-Zahlen und nebenbei eine kleine Tabelle nöthig ist, welche für die in den Determinanten vorkommenden Primzahlen α die Wurzeln der Congruenz $z^2 \equiv r\,(\alpha)$ angiebt.

Die Anzahl der benutzten Determinanten ist 170, davon sind 65 die von Euler sogenannten "numeri idonei;" von den übrigen finden sich einzelne in Legendre: Théorie des nombres oder sonstwie in mathematischen Zeitschriften. Die Mehrzahl derselben habe ich selbst fest stellen müssen.

* NOTE BY EDITOR.—The tables used by the author in the following examples do not appear in the present article. They have, however, been prepared, and, with some additional matter, will appear in a future number of the Journal.

BREMEN im August 1884.

Charaktere.								Formen.
+	+	+	+	—	—	—	—	
	.	.	.	.	.	.	.	1,1 1,2 1,4
	.	.	.	.	.	.	.	1,8 1,16
3	.	.	.	.	.	.	.	1,3 1,9
3	.	.	.	.	.	.	.	1,6 1,12
3	.	.	.	.	.	.	.	1,18 1,24
3	.	.	.	.	.	.	.	1,48 1,72
3	.	.	.	.	.	.	.	1,36 1,144 4,9 9,16
3	5	.	.	.	.	.	.	1,15 1,180 1,360 4,45 8,45
3	5	.	.	.	.	.	.	1,30 1,120
3	5	.	.	.	.	.	.	1,225 1,150 9,25 6,25
3	5	.	.	.	.	.	.	1,240 1,600 24,25
3	5	.	.	.	.	.	.	1,900 9,100 4,225 25,36
3	7	.	.	.	.	.	.	1,21 1,42
3	7	.	.	.	.	.	.	1,168 1,63 7,9
3	7	.	.	.	.	.	.	1,84 1,252 4,21 9,28
3	11	.	.	.	.	.	.	1,33 1,66 3,22
3	11	.	.	.	.	.	.	1,198 1,528 9,22 16,33
3	13	.	.	.	.	.	.	1,78 1,312
3	13	.	.	.	.	.	.	1,156 1,39 12,13 3,13
3	13	.	.	.	.	.	.	1,117 9,13
3	17	.	.	.	.	.	.	1,102 1,408
3	19	.	.	.	.	.	.	1,57
3	19	.	.	.	.	.	.	1,228 1,912 4,57 4,228
3	23	.	.	.	.	.	.	1,138 6,23
3	29	.	.	.	.	.	.	1,2088 9,232
3	31	.	.	.	.	.	.	1,93 1,372 4,93
3	37	.	.	.	.	.	.	1,333 9,37
3	43	.	.	.	.	.	.	1,258 6,43
3	47	.	.	.	.	.	.	1,282 3,94
3	59	.	.	.	.	.	.	1,177

Charaktere.								Formen.
+	+	+	+	—	—	—	—	
3	73	.	.	.	.	.	.	1,438 6,73
3	83	.	.	.	.	.	.	1,498 6,83
		.	.	3	.	.	.	2,9
	5	.	.	3	.	.	.	5,9 9,20 5,36
				3	5	.	.	3,5 2,15
				3	7	.	.	3,14
				3	11	.	.	2,33 6,11
				3	13	.	.	2,39
				3	17	.	.	6,17 17,24
				3	43	.	.	2,129 3,86
				3	83	.	.	2,249 6,83
3	5	7	.	.	.	.	.	1,105 1,525 21,25
3	5	7	.	.	.	.	.	1,1680 1,420 16,105 4,105
3	5	7	.	.	.	.	.	1,630 1,210 9,70
3	5	7	.	.	.	.	.	1,660 1,840 4,165
3	5	11	.	.	.	.	.	1,330 1,1320
3	5	11	.	.	.	.	.	1,165
3	5	13	.	.	.	.	.	1,390 1,1170 10,39 9,130
3	5	13	.	.	.	.	.	1,4680 9,520
3	5	17	.	.	.	.	.	1,510 1,765 15,34 9,85
3	5	19	.	.	.	.	.	1,1710 1,570 9,190 19,30
3	5	23	.	.	.	.	.	1,345
3	5	23	.	.	.	.	.	1,690 1,1380 6,115 4,345
3	5	29	.	.	.	.	.	1,3480 1,870 24,145 6,145
3	5	31	.	.	.	.	.	1,2790 9,310
3	5	37	.	.	.	.	.	1,1110 10,111
3	5	43	.	.	.	.	.	1,1290 1,5160 10,129 40,129
3	5	53	.	.	.	.	.	1,1590 10,159 6,265 15,106

Charaktere und binäre quadratische Formen für $N = 8n + 1$.

Charaktere.								Formen.
+	+	+	+	−	−	−	−	
3	.	.	.	5	7	.	.	7,90 3,70 10,63
3	.	.	.	5	11	.	.	10,33 33,40
3	.	.	.	5	19	.	.	3,190 10,57
3	.	.	.	5	29	.	.	10,87 15,58
3	.	.	.	5	43	.	.	3,430 30,43
3	7	13	.	.	.	.	.	1,1092 1,273 4,273
3	7	17	.	.	.	.	.	1,357
3	7	19	.	.	.	.	.	1,1197 1,798 9,133 7,114
3	7	31	.	.	.	.	.	1,1302 7,186
3	7	37	.	.	.	.	.	1,3108 21,148 4,777 37,84
3	7	37	.	.	.	.	.	1,777 21,37
3	.	.	.	7	11	.	.	7,66
3	.	.	.	7	13	.	.	13,21 13,84 21,52
3	11	13	.	.	.	.	.	1,858 3,286
3	11	17	.	.	.	.	.	1,1122 1,4488 33,34 33,136
3	11	97	.	.	.	.	.	1,6402 66,97 3,2134 22,191
3	.	.	.	11	17	.	.	6,187 22,51
3	13	43	.	.	.	.	.	1,1677 13,129
	.	.	.	.	.	.	.	1,6708 13,516 4,1677 52,129
3	13	61	.	.	.	.	.	1,7137 13,549 9,793 61,117
	5	.	.	3	7	.	.	5,21 6,35 5,84 20,21
	5	.	.	3	11	.	.	11,30
	5	.	.	3	13	.	.	6,35 15,26
	5	.	.	3	23	.	.	5,69 5,276 20,69
	5	.	.	3	37	.	.	6,185 15,74
	7	.	.	3	5	.	.	2,105 8,105
	7	.	.	3	11	.	.	2,231

Charaktere.								Formen.
+	+	+	+	−	−	−	−	
	11	.	.	3	5	.	.	5,33 3,110 5,132 20,33
	.	.	.	3	5	13	.	8,585 2,585 65,72 18,65
	17	.	.	3	5	.	.	2,255 17,30
	.	.	.	3	5	17	.	5,153 17,45
	.	.	.	3	5	19	.	2,855 18,95
	7	.	.	3	19	.	.	2,399 14,57
	11	.	.	3	7	.	.	14,33 33,56
	17	.	.	3	7	.	.	17,21
	11	.	.	3	13	.	.	11,78 26,33
	11	.	.	3	17	.	.	3,374 11,102
	17	.	.	3	11	.	.	2,561 8,561 17,66 17,264
5	.	.	.	.	.	.	.	1,5 1,25 1,100 4,25
5	7	.	.	.	.	.	.	1,70
5	11	.	.	.	.	.	.	1,220 5,44
5	13	.	.	.	.	.	.	1,130 1,520
5	17	.	.	.	.	.	.	1,340 4,85
5	19	.	.	.	.	.	.	1,190 1,760
5	29	.	.	.	.	.	.	1,145 5,29
5	29	.	.	.	.	.	.	4,145 5,116 1,580 20,29
5	31	.	.	.	.	.	.	1,310 10,31
5	41	.	.	.	.	.	.	1,205 5,41
5	89	.	.	.	.	.	.	1,445 5,89
5	101	.	.	.	.	.	.	1,505 5,101
5	101	.	.	.	.	.	.	1,2020 5,404 4,505 20,101
		.	.	5	7	.	.	7,10
		.	.	5	13	.	.	2,65 8,65
		.	.	5	17	.	.	5,68 5,17 17,20
		.	.	5	19	.	.	2,95

Charaktere.								Formen.
+	+	+	+	−	−	−	−	
5	7	11	.	.	.	.	.	1,385
5	7	31	.	.	.	.	.	1,2170 14,155
		11	.	5	7	.	.	5,77
		31	.	5	7	.	.	10,217 35,62
5	11	19	.	.	.	.	.	1,1045 5,209
5	11	19	.	.	.	.	.	1,4180 5,836 4,1045 20,209
5	13	29	.	.	.	.	.	1,1885 29,65
5	13	37	.	.	.	.	.	1,4810 26,185 10,481 65,74
5	13	37	.	.	.	.	.	1,19240 104,185 40,481 65,298
		29	.	5	13	.	.	5,377 13,145
7	.	.	.	.	.	.	.	1,7 1,28
7	.	.	.	.	.	.	.	1,112 1,14 2,7
7	11	.	.	.	.	.	.	1,154 11,14
7	19	.	.	.	.	.	.	1,133 1,532 4,133
7	37	.	.	.	.	.	.	1,1813 37,49
7	47	.	.	.	.	.	.	1,658 2,329
7	47	.	.	.	.	.	.	1,2632 8,329
7	113	.	.	.	.	.	.	1,1582 7,226 2,791 14,113
7	137	.	.	.	.	.	.	1,1918 7,274 2,959 14,137
7	11	13	.	.	.	.	.	1,2002 22,91
7	.	.	.	11	13	.	.	2,1001 11,182
11	.	.	.	.	.	.	.	1,22 1,88
11	23	.	.	.	.	.	.	1,253
13	.	.	.	.	.	.	.	1,13
13	17	.	.	.	.	.	.	1,442 1,1768 17,26 17,104
13	23	.	.	.	.	.	.	1,598 23,26
13	61	.	.	.	.	.	.	1,793 13,61
13	61	.	.	.	.	.	.	1,3172 13,244 4,793 52,61

Charaktere.								Formen.
+	+	+	+	−	−	−	−	
13	17	53	.	.	.	.	.	1,11713 17,689 13,901 53,221
17	.	.	.	.	.	.	.	1,34 1,36 2,17 8,17
23	.	.	.	.	.	.	.	1,46 2,23
29	.	.	.	.	.	.	.	1,58 1.232
31	41	.	.	.	.	.	.	1,2542 31,82 2,1271 41,62
37	.	.	.	.	.	.	.	1,37
41	.	.	.	.	.	.	.	1,82 1,328 2,41 8,41
71	.	.	.	.	.	.	.	1,142 2,71
3	5	7	11	.	.	.	.	1,3465 9,385
3	5	7	13	.	.	.	.	1,1365 1,5460 4,1365
3	5	7	17	.	.	.	.	1,1785 1,3570 21,85 51,70
3	5	7	17	.	.	.	.	1,7140 21,340 4,1785 84,85
3	5	7	23	.	.	.	.	1,19320 105,184
3	5	7	41	.	.	.	.	1,4305 21,205
3	5	.	.	7	17	.	.	6,595 34,105
3	7	11	29	.	.	.	.	1,13398 42,319 22,609 58,231
3	.	.	29	7	11	.	.	7,1914 33,406 6,2233 87,154
3	.	.	13	5	7	.	.	13,105
3	.	.	13	5	7	.	.	13,420 52,105
	5	7	.	3	.	.	13	21,65 21,260 65,84
	5	7	.	3	.	.	23	56,345 120,161
	7	17	.	3	5	.	.	2,1785 35,102
				3	5	7	11	5,693 45,77
				3	5	7	13	5,273 5,1092 20,273
				3	5	7	17	5,357 3,1190 17,105 17,210
				3	5	7	17	5,1428 68,105 20,357 17,420